Title (en)

Method for securing the transmission of short messages

Title (de)

Verfahren zur Sicherung der Übertragung von Kurznachrichten

Title (fr)

Méthode de sécurisation de la transmission de messages courts

Publication

EP 1569482 A1 20050831 (FR)

Application

EP 04100311 A 20040129

Priority

EP 04100311 A 20040129

Abstract (en)

The method involves requesting a public key (Kpu2) from one mobile equipment (EM2) by another mobile equipment (EM1). The key is received and stored in a temporary memory accompanied by identifier (ID2) of the equipment (EM2). A short messaging service (SMS) message is encrypted with the key. The encrypted message is received and decrypted by the equipment (EM2) with a private key (Kpr2) of the equipment (EM2). An independent claim is also included for a safety module for mobile equipment.

Abstract (fr)

Le but de la présente invention consiste à sécuriser la transmission des messages courts SMS via un réseau mobile afin d'empêcher leur capture et leur exploitation par des tiers. Ce but est atteint par une méthode de sécurisation de la transmission de messages courts (SMS) entre un premier et un second équipement mobile (EM1, EM2) via un réseau de communication mobile (NET) caractérisée en ce qu'elle est basée sur la cryptographie à clés asymétriques utilisant une clé publique (Kpu1, Kpu2) associée à une clé privée (Kpr1, Kpr2) propre à chaque équipement mobile (EM1, EM2) et comprend les étapes suivantes: requête de la clé publique (Kpu2) du second équipement (EM2) par le premier équipement mobile (EM1), réception et stockage de cette clé publique (Kpu2) dans une mémoire temporaire accompagnée de l'identifiant (ID2) du second équipement mobile (EM2), encryption du message court SMS avec ladite clé publique (Kpu2) reçue, transmission du message encrypté Kpu2(SMS) au second équipement mobile (EM2) via le réseau mobile (NET). réception et décryption du message (SMS, EMS) par le second équipement mobile (EM2) avec la clé privée (Kpr2) dudit second équipement (EM2). <IMAGE>

IPC 1-7

H04Q 7/38; H04Q 7/22

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/30** (2006.01); **H04L 29/06** (2006.01); **H04W 12/00** (2009.01)

CPC (source: EP)

H04L 9/08 (2013.01); **H04L 9/30** (2013.01); **H04L 63/0442** (2013.01); **H04L 63/0853** (2013.01); **H04W 12/037** (2021.01); H04W 4/14 (2013.01)

Citation (search report)

- [XY] US 6081601 A 20000627 - RAIVISTO TOMMI [FI]
- [X] US 2003078058 A1 20030424 - VATANEN HARRI [GB], et al
- [X] GB 2387505 A 20031015 - VODAFONE PLC [GB]
- [Y] SCHNEIER B: "Applied Cryptography", APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, 1996, pages 30 - 32, XP002966529, ISBN: 0-471-11709-9

Cited by

EP1830296A1; US9680803B2; US9848081B2; CN116915462A; EP2015553A1; EP2320618A1; FR2952211A1; FR2988248A1; US2011145564A1; EP3236429A1; FR3050301A1; US10917440B1; US9853926B2; US8325925B2; WO2009121046A1; US10395458B2; US10778658B1; US8225380B2; US10789594B2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

DOCDB simple family (publication)

EP 1569482 A1 20050831

DOCDB simple family (application)

EP 04100311 A 20040129